

PRIVACY CONDOMINIALE

PRIVACY-GDPR REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

A seguito dell'entrata in vigore del Regolamento Europeo n. 679/2016 cambiano le norme in materia di Privacy che regolano il trattamento dei dati personali.

Con questa normativa (immediatamente applicabile in Italia come in tutti i paesi facenti parte dell'UE) il legislatore europeo sottolinea l'importanza ed i rischi connessi all'utilizzo e al trattamento dei dati personali, siano essi sensibili o generici.

A partire dal 25 maggio 2018 sarà quindi direttamente applicabile anche in Italia il Regolamento UE 2016/679 (GDPR), in materia di protezione dei dati personali, con l'introduzione di significative novità che interessano professionisti ed imprese. Da tale data la gestione dei dati personali non sarà più solo un adempimento, ma diverrà un processo strutturale che incide sull'organizzazione di tutti gli operatori.

Con il Regolamento vengono introdotti nuovi diritti per gli interessati ma anche nuovi e più stringenti obblighi per tutti i soggetti che effettuano il trattamento del dato: tutti hanno l'obbligo di uniformarsi alla normativa, pena pesanti sanzioni.

Per chi tratta i dati, molte sono le novità introdotte, tra cui il dovere di effettuare un piano di valutazione del rischio, l'obbligo di redigere e tenere un Registro dell'attività del Trattamento o di monitorare costantemente l'attività di trattamento del dato e di segnalare entro 72 ore al Garante la possibile violazioni in materia di trattamento.

Di primaria rilevanza il principio di responsabilizzazione (accountability), che implica la libertà del titolare del trattamento nel predisporre misure preventive adeguate alla protezione dei dati personali, senza basarsi solamente su modelli precompilati ovvero documentazione standard: dunque, oltre a prevedere delle misure di base (in applicazione del principio denominato "privacy by default"), ciascun titolare del trattamento dovrà adottare delle procedure configurate specificamente sulle necessità e caratteristiche del trattamento svolto all'interno della propria realtà ("privacy by design").

Ogni soggetto deve comprovare il rispetto dei principi applicabili al trattamento dei dati personali, tramite vari adempimenti:

- aggiornamento dell'informativa sulla base degli artt. 13 e seguenti GDPR; il nuovo regolamento generale è molto più analitico nelle sue indicazioni, illustrando nel dettaglio gli adempimenti di legge a carico del titolare del trattamento. L'informativa deve essere chiara, onesta e compresa dalla persona cui è destinata, cioè l'interessato, che deve rilasciare il proprio consenso
- istituzione del registro dei trattamenti, nei casi previsti dall'art. 30 GDPR: esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10." L'istituzione e la tenuta del registro, in ogni caso, è fortemente consigliata dal Garante della privacy, perché consente una prima valutazione e diagnosi dei dati trattati all'interno della struttura
- designazione del DPO (Data Protection Officer), ove previsto dalla legge. La nomina non è obbligatoria, salvo che non si ricada nelle lett. B) e C) art. 37 GDPR, ossia se si effettuano trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala ovvero vengano trattati, sempre su larga scala, categorie particolari di dati personali (previsti agli artt. 9 e 10 del Regolamento, si tratta dei c.d. "dati particolari", ex "dati sensibili")
- verifica sulla necessità di procedere ad una valutazione di impatto privacy (DPIA) al fine di conoscere a fondo i processi di trattamento dei dati: in inglese "Data Protection Impact Assessment", introdotta dal nuovo Regolamento Europeo sulla Privacy che impone in capo al titolare del trattamento l'onere di effettuare una preliminare valutazione di impatto privacy
- verifica delle politiche interne in tema di trattamento dati, ai sensi dell'art. 24 GDPR, provvedendo a definire in maniera adeguata i ruoli e assicurandosi che tutto il personale riceva adeguata formazione
- verifica dei sistemi informatici per assicurare il rispetto dei principi di protezione dei dati
- formalizzare o rinnovare rapporti contrattuali con eventuali responsabili del trattamento dei dati, esterni o interni
- verifica sull'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio
- notifica di eventuali data breach, con specifiche procedure da attivare in caso di eventuali violazioni.

Ad oggi, il legislatore ha predisposto uno schema di decreto legislativo volto ad armonizzare la normativa interna con il Regolamento, tuttora in fase di approvazione, per cui quanto sopra potrà essere oggetto di successive integrazioni e/o modifiche.